sysdig

CASE STUDY

INFORMATIONS SUR L'ENTREPRISE :

Worldpay from FIS est un prestataire mondial de traitement et de services de paiements marchands, classé au Fortune 500.

BESOINS DE L'ENTREPRISE :

- Une plateforme de sécurité en libre-service et facile d'utilisation
- Une sécurité qui évolue avec FIS
- Une réduction de la lourdeur opérationnel
- Une uniformisation des normes PCI pour les marchands

DÉFIS :

- Un manque de visibilité évolutive dans les environnements cloud
- Une mauvaise compréhension de la gravité de la vulnérabilité et des mesures correctives
- Une absence de piste d'audit pour les dépannages et la conformité

IMPACT BUSINESS DE SYSDIG :

- Une amélioration de la communication entre les équipes de DevOps et de sécurité afin livrer plus rapidement des applications conformes aux normes PCI
- Une identification et une correction des vulnérabilités plus rapides pour éviter tout impact sur les clients

AVANTAGES DE LA PLATEFORME SYSDIG :

- Réduit les frais opérationnels de 50%
- Garantit une plus grande efficacité d'investigation avec les pistes d'audit
- Offre des résultats en quelques minutes avec une intégration rapide
- Réduit la maintenance avec une solution qui priorise le SaaS
- Simplifie l'obtention de la conformité PCI

INFRASTRUCTURE :

Multi Cloud - AWS, Azure et Google

ORCHESTRATION :

OpenShift de Red Hat

worldpay
from FIS

Worldpay acquiert un avantage concurrentiel grâce à une livraison plus rapide de solutions de paiement innovantes conformes aux normes PCI dans le monde entier

Présentation

Worldpay de FIS est l'un des plus importants prestataires mondiaux de traitement et de services de paiements marchands. Avec des milliards de transactions chaque année, Worldpay est présent dans 146 pays et regroupe plus de 300 modes de paiement dans 126 devises.

Son objectif est d'aider les marchands à utiliser les nouvelles technologies pour faire face aux défis relevés par les banques, aux paiements et aux investissements, tout en offrant des expériences hors pair à ses clients. Pour y parvenir, Worldpay construit des plateformes en libre-service hostées sur le cloud qui permettent aux marchands de travailler facilement.

Défi

En tant qu'acteur essentiel du secteur des paiements en constante évolution, Worldpay doit innover rapidement pour garder une longueur d'avance sur ses concurrents. Par exemple, avec l'apparition de la COVID-19 début 2020, les paiements sans contact (paiement vocal, paiements par reconnaissance

rétinienne et moyens de paiement numériques tels qu'UPI, AePS, etc.) sont très rapidement revenus sur le devant de la scène. Pour accélérer le développement d'applications permettant de faire face à la demande changeante, Worldpay utilise un environnement basé sur OpenShift de Red Hat, construit sur Kubernetes.

De par sa vocation d'aider les marchands à répondre aux normes PCI, il est extrêmement important pour Worldpay de garantir la disponibilité et la sécurité des applications. Les développeurs de l'entreprise doivent disposer d'une bonne visibilité sur leurs différents environnements, ce qui requiert une solution de sécurité et d'observabilité qui mette en évidence les problèmes potentiels dans les clusters et les clouds.

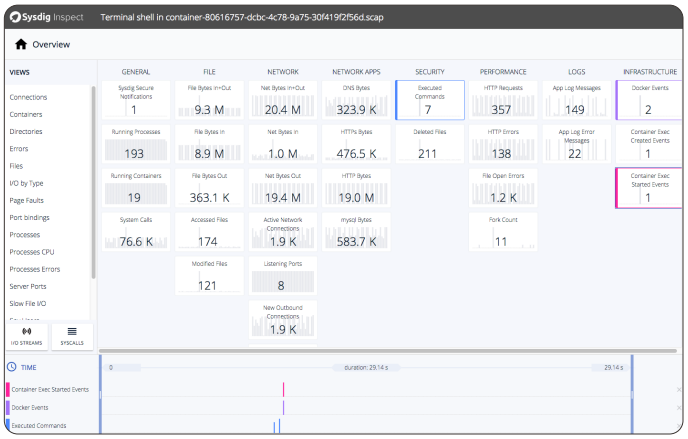
Selon Bernd Malmqvist, ingénieur principal de la plateforme de conteneurs à Worldpay, « Sysdig est devenu un élément essentiel de notre offre et il est formidable de constater qu'il a comblé les lacunes des deux côtés : il garantit la surveillance souhaitée par les équipes de développement, mais s'occupe également de la sécurité. Tout le monde a accès à Sysdig et l'utilise. »

Une réduction de 50 % des frais opérationnels

Worlpay aime l'approche de priorisation du SaaS de Sysdig. Comme Bernd l'explique, « nous souhaitons une utilisation 100 % sur le cloud. J'ai une infrastructure incroyablement dynamique, qui doit être constamment disponible. Il faut qu'elle puisse s'adapter et qu'elle évolue à l'échelle mondiale. Nous repoussons fortement les limites dans notre manière de construire et de livrer nos plateformes, et je pense que Sysdig s'intègre très bien dans ce genre de modèle avec son service de SaaS. Un centre de données local est trop contraignant et pas assez dynamique, particulièrement pour nous. Certains de nos clients n'ont pas d'accès direct à Internet et une solution locale est trop compliquée à gérer dans cette situation. »

Bernd poursuit : « Nous souhaitons consommer des services de SaaS dans la mesure du possible, car cela facilite grandement nos frais opérationnels, il nous suffit de laisser tourner un agent. Nous n'avons plus besoin de conserver le backend, donc nous pouvons nous concentrer principalement sur l'exécution de nos propres plateformes »

Selon Natnael Teferi, ingénieur principal de la sécurité chez FIS, grâce à la facilité d'intégration, à l'interface utilisateur intuitive, aux données détaillées et à l'offre SaaS, « Sysdig a réduit notre lourdeur opérationnelle de 50 %. » Sysdig est la seule solution de sécurité des conteneurs et Kubernetes construite dès le départ sous forme de solution de SaaS, ce qui la rend parfaite pour les entreprises en quête d'une flexibilité leur permettant d'innover rapidement. Selon Bernd, « nous essayons de parvenir à déployer ces clusters et à les utiliser sans effort, car ils sont capables de se gérer seuls. Sysdig nous permet d'y arriver. Sysdig repousse les limites, tout comme nous, en faisant constamment évoluer la feuille de route pour proposer de nouvelles fonctionnalités. Grâce à Sysdig, nous n'avons pas peur d'utiliser les nouvelles features disponibles. Nous n'avons pas à attendre qu'elles soient testées. Sysdig fait ce travail et nous avons confiance dans le produit. »



Une mise en conformité PCI simplifiée

En tant que plateforme de traitement des paiements, la conformité aux PCI est un enjeu majeur pour Worldpay. Lorsque les applications migrent vers le cloud, la multiplication des conteneurs et leur durée de vie réduite compliquent le respect des normes PCI. La validation de conformité est le principal obstacle à la livraison plus rapide des applications. Le non-respect des normes peut entraîner des sanctions financières importantes, mais surtout une perte de la confiance des clients et donc des revenus.

Bernd explique que « le respect du standard PCI est l'un des facteurs les plus compliqués à gérer dans l'exécution d'une plateforme Kubernetes au cœur d'un environnement très sécurisé. Sysdig nous a facilité les choses en réduisant les efforts que nous devions fournir en simplifiant le respect des contraintes PCI. La construction d'une plateforme sécurisée demande beaucoup de travail, mais Sysdig nous a permis de traiter rapidement certains éléments clés tels que la prévention, l'analyse de l'exécution, la détection des intrusions, le scan des vulnérabilités.

La sécurité, le DevOps et les opérations travaillent en parfaite collaboration

Exécuter des conteneurs dans un environnement de production implique que la sécurité et la visibilité s'intègrent dans les flux de travail existants. Sysdig est la seule solution capable de traiter les cas d'utilisation liés à la sécurité, à la conformité et à la surveillance grâce à un agent et à un backend unique. Cet aspect était très important aux yeux de Worldpay.

Au-delà de la consolidation des outils et des économies, Worldpay est en mesure de traiter plusieurs cas d'usages avec des ressources limitées.

Selon Natnael, « comme nous exécutons une plateforme distribuée, il est formidable de pouvoir compter sur un outil unique capable de traiter plusieurs cas d'usages liés à la sécurité et à la surveillance. L'agent unique non intrusif signifie que nous n'avons pas plusieurs agents susceptibles d'interférer les uns avec les autres. »

> **« Avec les logs d'audit dans nos buckets S3, nous pouvons revenir en arrière et voir ce qui s'est passé si un attaquant est allé sur la plateforme. Nous pouvons également vérifier s'il a récupéré quelque chose et/ou la manière dont il y a accédé. Ces informations constituent un gain de temps important, car sans les logs d'audit il est impossible de savoir ce qui s'est passé. Les autres solutions ne proposent pas ce service.. »**
>
> **- Natnael Teferi**
> **Lead DevSecOps Cloud Security Architect**

Bernd explique que son « équipe collabore très étroitement avec l'équipe de Natnael. Alors, j'ai été très impressionné par le fait de disposer de Sysdig Monitor et de Sysdig Secure sans avoir à ajouter d'agent supplémentaire. Par le passé, Worldpay utilisait d'autres solutions très intrusives sur une plateforme OpenShift et nous avons eu des problèmes. Je pense qu'il est très important de disposer de cet agent unique et non intrusif. »

Prêt à l'emploi en 30 minutes

Étant donné que les développeurs du monde entier utilisent les plateformes en libre-service de Worldpay, il est extrêmement important de pouvoir intégrer des

outils efficaces rapidement ; après tout, le temps c'est de l'argent. L'un des aspects que des clients comme Worldpay aiment chez Sysdig, c'est la rapidité avec laquelle ils peuvent procéder à l'intégration et obtenir des résultats.

Selon Natnael, « il est rapide et facile d'installer Sysdig. Il n'est pas nécessaire d'installer une interface graphique ou d'ouvrir des ports sur le pare-feu, ce qui est coûteux avec ce type de structure. Il ne nous a pas fallu plus de 30 minutes pour mettre en place le SaaS de Sysdig et obtenir les métriques du premier cluster. Cela nous avait pris un mois pour en arriver au même point avec les autres outils que nous avions utilisés par le passé. Sysdig contient de formidables politiques prêtes à l'emploi, ce qui permet un gain de temps considérable. »

Le plugin Sysdig Teams, facile à utiliser, permet aux administrateurs de configurer les accès, ce qui est important pour Natnael. « Une fois l'installation terminée, lorsque nous ajoutons de nouvelles équipes qui doivent pouvoir bénéficier d'un accès, il nous suffit d'assigner un responsable d'équipe. Ce dernier peut alors définir les accès et gérer ses équipes, ce qui nous permet là encore de faire des économies. Les gens ne perdent pas leur temps à solliciter des accès et des identifiants, mais ils vont voir leur responsable d'équipe qui s'occupe de gérer les différents accès. »

Travaillez à générer des revenus, pas à gérer les risques

Selon Bernd, Sysdig n'encombre pas son équipe et ses clients d'informations inutiles. Il préfère s'employer à afficher uniquement les données importantes. « Lorsque vous utilisez un outil de sécurité de conteneurs, tout le monde sait qu'une fois qu'il est déployé et connecté au backend, vous vous connectez et vous recevez aussitôt d'innombrables informations pour

vous dire que vos conteneurs sont tous vulnérables. C'est vraiment démoralisant et vous ne savez pas par où commencer. Ce que j'aime avec Sysdig, c'est que lorsque vous vous connectez, presque tout s'affiche en vert. Je m'intéresse généralement aux vulnérabilités élevées ou graves et c'est exactement ce que Sysdig affiche lorsque vous utilisez les tableaux de bord. Il est également facile d'obtenir toutes les informations relatives aux vulnérabilités secondaires, mais la plupart du temps ce n'est pas ce qui vous intéresse, n'est-ce pas ? Donc je ne veux pas perdre mon temps avec ça. Je veux juste voir les incidents dont je devrais me préoccuper et c'est exactement ce que Sysdig affiche. »

Natnael ajoute que « d'un point de vue sécuritaire, si vous voyez plusieurs vulnérabilités et que vous travaillez en mode agile, des heures spécifiques sont prévues dans la semaine pour résoudre ces vulnérabilités. Si mon équipe se connecte et voit 500 vulnérabilités, elle se dit "est-ce que je vais résoudre nos vulnérabilités ou prendre le temps de développer quelque chose qui générera de l'argent ?" Sysdig vous indiquera les vulnérabilités pour lesquelles des solutions sont disponibles. C'est vraiment utile ; mon équipe peut facilement réparer la situation et passer à autre chose. Le fait d'afficher les éléments importants

et la manière de les résoudre est essentiel pour réduire le risque. L'outil nous fait gagner du temps. »

Pour ce qui est de la mise en place de politiques de gestion des risques, Natnael explique que « grâce à la fonction de politique sur l'exécution de Sysdig, nous pouvons facilement créer une politique et cela entraîne immédiatement une alerte de notification. Cela simplifie notre travail sur les politiques et le déploiement. Il nous suffit de créer une sorte de Daemonset. Cet aspect, ainsi que les conseils de Sysdig qui expliquent comment déployer différents scénarios, facilitent grandement la gestion du risque. »

Compatibilité totale avec Prometheus

De nombreux développeurs commencent à travailler avec le système open source Prometheus, afin d'obtenir des métriques clés pour les services cloud-native. Toutefois, s'adapter à la production avec de multiples clusters Kubernetes exige de multiples serveurs Prometheus, ce qui rend l'observation de tendances difficile. Les problèmes avec les microservices ayant des dépendances entre les plateformes peuvent facilement passer inaperçus. Pour Worldpay, l'utilisation de Prometheus et du langage de requête PromQL par Sysdig est un grand avantage.

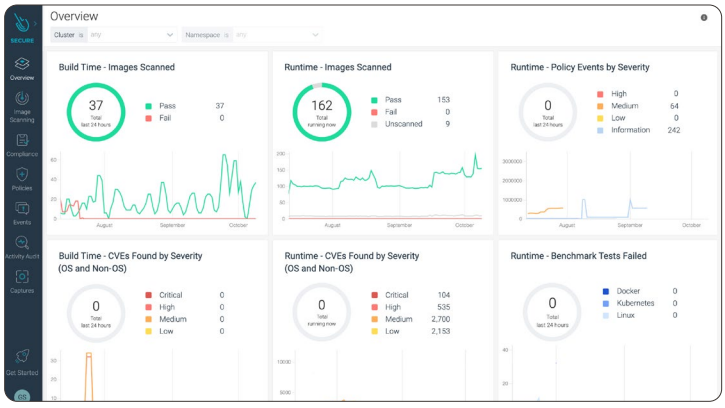
Selon Bernd, « mon équipe est très contente de travailler avec Sysdig car nous utilisons énormément Prometheus, et elle apprécie l'assistance de Sysdig pour PromQL. C'est réellement un élément essentiel pour nous. Nous avons construit énormément de KPI autour de Prometheus et, grâce à Sysdig, nous pouvons vraiment utiliser ces métriques.

Nos projets futurs incluent la livraison continue avec des mises en œuvre multirégionales et là, Prometheus aura vraiment un rôle prépondérant. Le support de Sysdig pour Prometheus est unique et constitue sans aucun doute l'un des principaux éléments qui nous aidera à construire plus d'outils autour de ces plateformes. »

Les logs d'audit font des investigations une réalité pour la première fois

Lorsqu'une réponse à un incident est requise pour Kubernetes, les équipes SOC doivent pouvoir analyser une liste interminable de scénarios. Dans les environnements de conteneurs, lorsqu'un conteneur n'existe plus, les données inhérentes disparaissent également, ce qui rend l'investigation pratiquement impossible. La disponibilité des données qui permet d'accélérer la réponse en cas d'incident est une garantie sans pareille en cas de problème. « La fonction d'investigation a joué un rôle essentiel dans notre choix de Sysdig pour gérer la sécurité. Avec les logs d'audit dans nos buckets S3, nous pouvons revenir en arrière et voir ce qui s'est passé si un attaquant est allé sur la plateforme. Nous pouvons également vérifier s'il a récupéré quelque chose et/ou la manière dont il y a accédé. Ces informations constituent un gain de temps important, car sans les logs d'audit il est impossible de savoir ce qui s'est passé. Les autres solutions ne proposent pas ce service. En outre, Sysdig aide à

> **« Nous essayons de parvenir à déployer ces clusters et à les utiliser sans effort, car ils sont capables de se gérer seuls. Sysdig nous permet d'y arriver. »**
>
> **- Bernd Malmqvist**
> **Principal Container Platform Engineer, Worldpay**



identifier les personnes à informer et tire des enseignements de la configuration », ajoute Natnael.

Natnael poursuit : « Le cycle de vie du conteneur se mesure en secondes, et il existe de nombreuses manières de faire les choses, particulièrement pour l'équipe de sécurité. Nous devons pouvoir avoir confiance en la sécurité et de l'intégrité des conteneurs qui peuvent être en ligne pendant quelques secondes, ou peut-être quelques semaines, avant de disparaître. Grâce à Sysdig, nous disposons d'une visibilité en temps réel sur la totalité de l'environnement FIS. Et en cas de problème, nous disposons de ces données pour procéder à une investigation. »

Avec Sysdig, le multi cloud est une réalité

Entre FIS et Worldpay, l'infrastructure qui soutient leurs applications comprend plusieurs clouds. Selon Natnael, « avec FIS, nous utilisons Azure et certains environnements Google Cloud. Worldpay repose sur des environnements AWS. Sysdig sécurise et surveille ces divers clouds. Avec l'expansion de l'entreprise, Sysdig joue un rôle important car il soutient toutes les plateformes. Si FIS achète une autre entreprise dans quelques années, nous n'aurons aucun problème à étendre notre outil Sysdig de sécurité et de surveillance pour inclure cette nouvelle entreprise. À mon avis, c'est un aspect très important car nous n'aurons pas besoin de mettre en œuvre, de déployer et d'autres outils. »

Sysdig est un membre actif de la communauté open source

Sysdig est une entreprise basée sur l'open source qui a apporté plusieurs produits à la communauté, notamment Falco, le projet cloud-native de facto de sécurité d'exécution, adopté par la CNCF. Sysdig contribue à définir les meilleures pratiques et à aider la communauté. La construction en open source permet également à Sysdig d'innover plus rapidement.

Bernd ajoute : « j'aime vraiment que Sysdig soit aussi actif avec l'open source. Sysdig possède des projets en open source pour la sécurité et la surveillance. Les gens peuvent déployer les deux et les exécuter gratuitement. Il y a également une version pour les entreprises qui s'intègre parfaitement une fois que vous adoptez les outils open source. S'il vous faut plus de capacités et de fonctionnalités, Sysdig est là pour vous. Se comporter en bon membre de la communauté et en meneur est important à mes yeux. »

Pour en savoir plus sur Sysdig, rendez-vous sur www.sysdig.com et pour bénéficier d'un essai gratuit, rendez-vous sur www.sysdig.com/trial.

CS-WORLDPAY-FR Rev. A 10/21